Configure User RBAC for the Oxidized or RANCID Network Device Configuration Backup Tools on Cisco Nexus Devices

Contents

Introduction

This document describes how to configure local user accounts on Cisco Nexus devices to use Role-Based Access Control (RBAC) roles that are restricted to commands used by the Oxidized or RANCID network device configuration backup tools.

Prerequisites

Requirements

You must have access to at least one user account that can create other local user accounts and RBAC roles. Typically, this user account holds the default "network-admin" role, but the applicable role might be different for your particular network environment and configuration.

Cisco recommends that you have knowledge of these topics:

- How to configure user accounts in NX-OS
- How to configure RBAC roles in NX-OS
- How to configure your network device configuration backup tool

Components Used

The information in this document is based on these software and hardware versions:

- Nexus 9000 platform NX-OS Release 7.0(3)I7(1) or later

The information in this document covers these network device configuration backup tools:

- Oxidized v0.26.3
- RANCID v3.9

The information in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

This section provides configuration instructions for the Oxidized and RANCID network device configuration backup tools.

> **Note**: If you use a different network device configuration backup tool, use the Oxidized and RANCID procedures as examples and modify the instructions as appropriate for your situation.

Configure User Account and Role for Oxidized

As seen in Oxidized's NX-OS model, Oxidized executes this list of commands by default on any Cisco Nexus device that runs NX-OS:

- terminal length 0
- show version
- show inventory
- show running-config

To configure a user account that is allowed to execute only those commands, perform this procedure:

1. Configure an RBAC role that permits those commands. In the below example, "oxidized" is defined as the role name.

```
Nexus# configure terminal
Nexus(config)# role name oxidized
Nexus(config-role)# description Role for Oxidized network device configuration backup tool
Nexus(config-role)# rule 1 permit command terminal length 0
Nexus(config-role)# rule 2 permit command show version
Nexus(config-role)# rule 3 permit command show inventory
Nexus(config-role)# rule 4 permit command show running-config
Nexus(config-role)# end
Nexus#
```

> **Caution**: Do not forget to add a rule that permits the **terminal length 0** command as shown in the example above. If this command is not permitted, then the Oxidized user account will receive a "% Permission denied for the role" error message when it executes the **terminal length 0** command. If the output of a command executed by Oxidized exceeds the default terminal length of 24, Oxidized will not gracefully handle the "--More--" prompt (demonstrated below) and will raise a "Timeout::Error with msg 'execution expired'" warning syslog after it executes commands on the device.

```
Nexus# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
```

```
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.35
  NXOS: version 7.0(3)I7(6)
--More--    <<<
```

2. Configure a new user account that inherits the role you configured in step 1. In the below example, this user account is named "oxidized" and has a password of "oxidized!123".
```
Nexus# configure terminal
Nexus(config)# username oxidized role oxidized password oxidized!123
Nexus(config)# end
Nexus#
```

3. Manually log in to the Nexus device with the new Oxidized user account and verify that you can execute all the necessary commands without issue.
4. Modify Oxidized's input data source to accept the account credentials of the new Oxidized user account. Sample output of a CSV source is shown below with five Nexus devices.
```
nexus01.local:192.0.2.1:nxos:oxidized:oxidized!123
nexus02.local:192.0.2.2:nxos:oxidized:oxidized!123
nexus03.local:192.0.2.3:nxos:oxidized:oxidized!123
nexus04.local:192.0.2.4:nxos:oxidized:oxidized!123
nexus05.local:192.0.2.5:nxos:oxidized:oxidized!123
```

   The relevant Oxidized source configuration for the above CSV source is shown below.
```
---
source:
  default: csv
  csv:
    file: "/filepath/to/router.db"
    delimiter: !ruby/regexp /:/
    map:
      name: 0
      ip: 1
      model: 2
      username: 3
      password: 4
```
5. Execute Oxidized against the configuration file and data source and verify that the output of all commands appears in your configured data output. The specific command to do this will depend upon your implementation and installation of Oxidized.

Configure User Account and Role for RANCID

As seen in RANCID's NX-OS model, RANCID executes this list of commands by default on any

Cisco Nexus device that runs NX-OS:

- terminal no monitor-force
- show version
- show version build-info all
- show license
- show license usage
- show license host-id
- show system redundancy status
- show environment clock
- show environment fan
- show environment fex all fan
- show environment temperature
- show environment power
- show boot
- dir bootflash:
- dir debug:
- dir logflash:
- dir slot0:
- dir usb1:
- dir usb2:
- dir volatile:
- show module
- show module xbar
- show inventory
- show interface transceiver
- show vtp status
- show vlan
- show debug
- show cores vdc-all
- show processes log vdc-all
- show module fex
- show fex
- show running-config

Some of the commands in this list can be executed only by user accounts that hold the network-admin user role. Even if the command is explicitly permitted by a custom user role, user accounts that hold that role might not be able to execute the command and will return a "%Permission denied for the role" error message. This limitation is documented in the "Configuring User Accounts and RBAC" chapter of each Nexus platform's Security Configuration Guide:

> *"Regardless of the read-write rule configured for a user role, some commands can be executed only through the predefined network-admin role."*

As a result of this limitation, RANCID's default command list requires that the "network-admin" role is assigned to the NX-OS user account used by RANCID. To configure this user account, perform this procedure:

1. Configure a new user account with the "network-admin" role. In the below example, this user account is named "rancid" and has a password of "rancid!123".

```
Nexus# configure terminal
Nexus(config)# username rancid role network-admin password rancid!123
Nexus(config)# end
Nexus#
```

2. Manually log in to the Nexus device with the new RANCID user account and verify that you can execute all the necessary commands without issue.
3. Modify RANCID's login configuration file to use the new user account. The procedure to modify the login configuration file varies from one environment to another, so details are not provided here. **Note**: RANCID's login configuration file is typically named **.cloginrc**, but your deployment of RANCID might use a different name.
4. Execute RANCID against a single Nexus device or set of devices and verify that all commands execute successfully. The specific command to do this depends upon your implementation and installation of RANCID.

   Note: If the Nexus user account that is used by RANCID absolutely cannot hold the "network-admin" role for security reasons and if the relevant commands that require this role are not necessary in your environment, you can manually remove those commands from the list that is executed by RANCID. First, execute the full list of commands shown above from a Nexus user account that is only permitted to run the aforementioned commands. The commands that require the "network-admin" role will return a "%Permission denied for the role" error message. You can then manually remove the commands that returned the error message from the list of commands executed by RANCID. The exact procedure to remove those commands is outside the scope of this document.

Verify

There is currently no verification procedure available for this configuration.

Troubleshooting

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Oxidized GitHub Project**
- **RANCID (Really Awesome New Cisco Conflg Differ) Homepage**

- **"Configuring User Accounts and RBAC" chapter of Cisco Nexus 9000 Series NX-OS Security Configuration Guide:**
  - **Release 9.3(x)**
  - **Release 9.2(x)**
  - **Release 7.x**
  - **Release 6.x**
- **"Configuring User Accounts and RBAC" chapter of Cisco Nexus 7000 Series NX-OS Security Configuration Guide:**
  - **Release 8.x**
  - **Release 7.x**

    - Release 6.x
- "Configuring User Accounts and RBAC" chapter of Cisco Nexus 6000 Series NX-OS System Management Configuration Guide
    - Release 7.x
    - Release 6.x
- "Configuring User Accounts and RBAC" chapter of Cisco Nexus 5600 Series NX-OS System Management Configuration Guide
    - Release 7.x
- "Configuring User Accounts and RBAC" chapter of Cisco Nexus 5500 Series NX-OS System Management Configuration Guide
    - Release 7.x
    - Release 6.x
- Technical Support & Documentation - Cisco Systems